



INTERNAL AUDIT REPORT

Office of Technology and Information Services Student Information Systems



May 14, 2002

Roanoke City School Board Audit Committee
Roanoke, Virginia

We have completed an audit of the student information system. The audit was performed in accordance with generally accepted government auditing standards.

BACKGROUND

Roanoke City Public Schools implemented the Pentamation student information system in July 2000. Pentamation is a real-time application that is used to manage student demographics, daily attendance, class attendance, scheduling, and grades.

The Pentamation system has three modules: the open series module, graphical student management system (GSMS) module, and the Cognos module. The open series runs on a UNIX server and has menus, help screens, user-defined tables and fields, and a relational database for direct access to student data in the system through query and user-defined reports. The GSMS and Cognos run on NT servers that interface with the relational database on the UNIX server. GSMS is designed for the windows environment and allows the user to view information from multiple Open Series applications for the same student. It provides a quick way to view an individual student's performance. Cognos is a report writer package that can be used to develop custom reports.

Every school uses the demographic and daily attendance features of Pentamation. Raleigh Court Elementary and all of the middle and high schools use the scheduling and grading features. Only Patrick Henry High School and William Fleming High School use the class attendance feature.

The Student Information Systems Coordinator, Carole Smith, is the primary contact between the school system and Pentamation. She is the only person in the Office of Technology and Information Services dedicated to administering the Pentamation system. Ms. Smith trains school staff and administrators on how to use the Pentamation software and she also responds to users' calls for assistance. While Ms. Smith is the primary administrator of the system, there are three people within the Office of Technology with database administrator access rights. These staff members also respond to users' requests for assistance. The Office of Technology does not keep a

record of calls for help but estimates three to four hours of staff time per day is used to respond to Pentamation calls. Pentamation also has a toll free support line and a knowledge base on their web site that the Office of Technology can access if they are unable to resolve a user's problem. There are approximately 290 users with access to the Pentamation system.

OBJECTIVES

The specific objectives of the audit were as follows:

- To evaluate the design and effectiveness of the system of internal controls to ensure system administration and security administration are properly managed.
- To evaluate the design and effectiveness of the system of controls to ensure accurate student demographic, enrollment, attendance, and grade data is captured and reported.
- To verify compliance with certain Virginia Board of Education regulations regarding the management of student data.
 - Monitoring of student aggregate days attendance
 - Withdrawing pupils absent for 15 consecutive days or more
 - Retention of student records at the schools
 - Annual notification of parent(s) regarding rights to access student records

We completed test work at the following schools: Patrick Henry, William Fleming, Addison Middle, Breckinridge Middle, Ruffner Middle, Raleigh Court Elementary, Lincoln Terrace Elementary, and Fallon Park Elementary.

METHODOLOGY

We gained an understanding of the student information system through interviews with staff and administrators in the Office of Technology and the schools. We reviewed the Roanoke City School Board policy manual and the Virginia Board of Education regulations regarding the management of student data. Based on this information, we developed tests to evaluate the operation and effectiveness of controls.

SCOPE

The audit focused on the system of internal controls in place as of January 31, 2002. We tested data generated between July 1, 2001 and March 31, 2002. Due to time constraints, we limited our testing of student grades to verifying that grades were reviewed and corrections were entered into Pentamation. We did not evaluate the underlying documents that support the grades recorded on Pentamation.

RESULTS

The Pentamation users spoke very highly of the support provided by Ms. Smith and the other staff in the Office of Technology. We found that system backup and environmental controls were in place in the Office of Technology. At the schools we found that the staff had a good understanding of the system and were utilizing Pentamation as intended.

When reviewing a new system it is common to identify areas for improvement. The following findings are the issues we evaluated to be most significant in nature. Less significant issues were shared with management during our closing conference.

Finding 01

We selected a sample of 160 student emergency cards and found that 27 (16.9%) were not on file. Of the remaining emergency cards, 41 (25%) had telephone, address, and/or guardian demographic information that did not agree with the information on the Pentamation system. School staff could have a difficult time contacting a parent or guardian if the Pentamation system was unavailable and an emergency card was not on file. The inconsistency of information that is on emergency cards versus the Pentamation system could add to the time it takes to contact parents or guardians in an emergency.

Recommendation 01

The Central Administration took steps to address this concern as soon as the preliminary findings were reviewed with them. We have no recommendations beyond management's current response.

Management Response 01

The administrative instructional and technology staff will continue to address this issue through on-going training, reminders via memo to principals and clerical staff, and through periodic meetings. Principals are strongly encouraged to build this aspect into any future employee evaluations.

Additionally, the Office of Technology will use selected central office staff to conduct internal audits at school sites on a periodic basis.

Finding 02

The Virginia Board of Education's regulation VAC 20-110-100 states that a pupil shall be dropped from the roll and marked "withdrawn" once that pupil has been absent for 15 consecutive days or more. In such cases, Roanoke City Public School's policy is to record the date of the student's 16th consecutive absence as the effective withdrawal date. We selected 40 students that had been absent for 15 consecutive days or more based on Pentamation records. We found that 15 of the 40 students sampled had effective withdrawal dates that were past the date of their 16th consecutive absence.

Many of the effective dates entered exceeded the correct date by just a few days. In some cases, the effective date was significantly later than the date of the 16th consecutive absence. One student's attendance records showed that the effective withdrawal date should have been 12/13/01 but the effective date entered on the system was 1/31/02. In three other cases, the effective withdrawal date should have been entered in February 2002 but the students were still enrolled when we tested the records in late March. In a separate test, we noted one student that had a notation by her name that she was a "no show", however; she was never marked absent. This notation went unnoticed the entire school year until noted during our test work. The results of our testing indicate that average daily membership and average daily attendance may be slightly inflated.

Recommendation 02

We recommend that school administrators assign the responsibility for withdrawing students who miss 15 consecutive days to one person. A staff person who works with student guidance or truancy would seem to be in the best position to know if a student should be withdrawn due to absences. The Pentamation system has a report showing students absent for 15 or more consecutive days. We recommend that the Principal or Assistant Principal run and review this report weekly to confirm withdrawals are processed according to regulation.

Management Response 02

The administration will strongly encourage school administrators to limit the responsibility for withdrawing students who miss 15 consecutive days to one individual. A person at each site will be cross-trained to run the 15-day report as well. The Office of Technology will continue to remind the Principal and Assistant Principal about running and reviewing the appropriate weekly absence report. Selected central office personnel will run the report on a regular basis and check withdrawal dates of W9 students.

Finding 03

We noted that 18 out of 182 (9.9%) teacher grade change requests we reviewed were not entered into the Pentamation system. We believe the requests were either overlooked or misinterpreted by the staff entering grades. In each case, the student either received an inaccurate grade or did not receive a grade, which could affect the student's GPA and class rank.

Recommendation 03

In general, the schools have satisfactory procedures in place for teachers to verify grades before final report cards are printed. The errors are a result of a break down in communication between the data entry personnel and the teachers. We recommend that school administrators emphasize the importance of communication between those entering corrections and the teachers. Secretaries or other administrative staff that post

grade corrections should be instructed to clarify changes with the teachers if notations are in any way unclear or out of the ordinary.

Management Response 03

The administration will continue to emphasize the importance of accuracy of grade verification and communication between teachers and data entry personnel. The Office of Technology will provide assistance to school administrative staff to develop formalized processes for grade verification where needed.

Finding 04

The Office of Technology assigns user names and passwords as they setup users on the Pentamation system. The users do not have the ability to change their passwords themselves. The Office of Technology has recorded the user names, IDs, and passwords in an excel file to monitor who has access to the Pentamation system and to provide Pentamation users with their passwords if they forget their password. The resulting effect is that security over access to student information is weakened because the users cannot be held accountable for activity that may occur under their user IDs. This significantly increases the risk that inappropriate and unauthorized changes could be made to student records.

Recommendation 04

We recommend that the Office of Technology remove the users' passwords from its excel spreadsheet because when passwords are known to more than one person, the responsibility of the user for all activity within their account cannot be enforced.

Based on our discussions with the Director and staff in the Office of Technology, there are server issues that make it difficult to efficiently incorporate user control over passwords into their security administration process. Both of our offices have contacted other Pentamation users, as well as the application and server vendors, in an effort to develop an agreeable solution. The solution must move control over the password to the user and eliminate any possibility that other people will learn the password through no fault of the user.

Management Response 04

The Office of Technology is working with technical support from Pentamation and the City's Department of Technology to resolve this issue as soon as feasibly possible. The Microsoft Excel spreadsheet containing Pentamation passwords has been erased. Software is being investigated that will synchronize password changes for users within the NT and Unix environments.

Finding 05

We evaluated the user access list (excel file) and found that five user ids were identified as being active on the Pentamation system and not listed in the access list and four terminated users were active on the Pentamation system and not listed in the access list. With an incomplete user access list and active terminated employee ids on the Pentamation system, terminated employee ids could be used to gain access to the Pentamation system.

Recommendation 05

Adopt formal processes to add and remove employees from the Pentamation system in order to maintain a current and accurate listing of users. The Office of Technology should create a System Request Access form for the data owners (i.e. principals) to complete when they have a new hire that needs access to the Pentamation system. The data owners should be responsible for determining and documenting the users access rights to the Pentamation system.

The data from the System Request Access form should be used by The Office of Technology to set up the user's access rights. In addition The Office of Technology should use the form as a checklist to ensure the new user id was added to the applicable servers and the user access list in MS Excel.

The Office of Technology has also created a User Agreement form that users will sign that specifies the user's responsibilities. We believe this will strengthen the user set-up and removal processes and is a significant improvement to their system of controls.

Management Response 05

The Office of Technology will establish a formal process between the Office of Technology and HRD to report and record changes in administrative and clerical status. A new Pentamation User Agreement will be used to specify the user's rights and responsibilities relative to the student information system. This form will be filed on a yearly basis for all personnel using Open Series and GSMS.

Finding 06

Four user IDs setup by Pentamation during the installation of the system in July 2000 have database administrator rights. This level of access allows the vendor to view and modify application logic and student information in the system. This increases the risk that application logic and student information could inadvertently be altered.

Recommendation 06

Standards for security administration state that system access should be limited to a minimum number of vendor staff and that the access should be the least needed. We

recommend that the Office of Technology reduce the number of vendor accounts and limit the vendor's access to the least needed to perform their support and maintenance functions.

Management Response 06

The Office of Technology has removed the database rights for two of the vendor accounts.

Finding 07

We reviewed certain higher risk access rights to determine if access was limited to the user's home building or school as would be expected. Our tests yielded the following results:

- We found that 112 of the 141 users with the ability to change and enter students' daily attendance data could do so at more than one school.
- We found that 6 of the 9 users with the ability to change historical grades and courses could do so at more than one school.
- We found that 49 of the 54 users with the ability to enter information related to student discipline actions could do so at more than one school.

There are over 300 access rights that can be granted to a user and each of these rights can be granted for a school or school group. The school group field was thought to default to a user's home school if left blank when in fact the default access was all schools. The Office of Technology has reviewed user accounts and entered users' home schools in the school group field.

Recommendation 07

We recommend that the Office of Technology provide its staff with additional Pentamotion security training. We also recommend that the Office of Technology emphasize security administration and develop more detailed procedures for requesting and granting access. User access requests should be balanced against the security interests served by limiting access. Access to all users should be granted on a "need to know, need to do basis".

Management Response 07

The Office of Technology has reviewed the rights of all users and security has been tightened on a "need to know" and "need to do" basis. Additional security training will be conducted to staff and emphasis will be given to security administration.

Finding 08

The firewall and server logs were not activated and as a result were not being monitored for attempted access violations to the Pentamation system. Unauthorized attempts to access student information would go undetected. This increases the risk that an individual could gain unauthorized access to student information on the Pentamation system.

Recommendation 08

The Office of Technology activated the logs as soon as our department noted the concern. We recommend that they develop a meaningful process for monitoring the logs, either based on frequent scans of the reports for unusual activity or some type of exception reporting.

Management Response 08

The firewall and server logs have been activated and procedures have been adopted to monitor the logs.

CONCLUSION

Based on the results of our audit work, we conclude that system administration and security administration functions can be enhanced to provide greater assurance that student information is secure. We also conclude that procedures for collecting, processing, and reporting student information at the schools should be improved to provide greater assurance that information is accurate and available. We also conclude that the schools tested have substantially complied with Virginia Board of Education regulations regarding the management of student data.

We would like to thank the Office of Technology, Central Administration, and the staff and administrators at the schools for their cooperation and assistance during the audit.

Pamela Mosdell
Senior Auditor

Drew Harmon, CPA, CIA
Municipal Auditor